Il protocollo IP

Affrontiamo ora una dei due componenti di TCP/IP: il protocollo IP. Una buona comprensione di IP è necessaria per proseguire con TCP e UDP, poiché IP è il componente che tratta il trasferimento dei datagrammi lungo la rete. IP è l'elemento essenziale che impacchetta i dati e li invia a destinazione.

Internet Protocol

IP è un protocollo primario del modello OSI, così come una parte integrante del TCP/IP. Sebbene la parola Internet sia utilizzata nel nome del protocollo, il suo uso non è ristretto ad Internet. E' vero che tutte le macchine collegate alla rete utilizzano o comprendono IP, ma esso può essere usato in reti dedicate che non hanno alcun collegamento con Internet. IP è una scelta davvero buona per ogni rete che necessita di un efficiente protocollo per comunicazioni macchina-macchina.

Il compito principale di IP è l'indirizzamento di datagrammi di informazioni tra computer e il controllo del processo di frammentazione di questi datagrammi. Il protocollo possiede una definizione formale della struttura di un datagramma e della formazione di un header composto di informazioni relative al datagramma. IP è responsabile dell'instradamento del datagramma , determinando dove verrà inviato, e individuando percorsi alternativi in caso di problemi.

Un altro importante aspetto di IP è relativo alla consegna inaffidabile di datagrammi. IP non ha nulla a che fare con il controllo dei flussi d'informazioni o l'affidabilità: non ha alcuna capacità interna per controllare che un messaggio inviato sia correttamente ricevuto: IP non ha un checksum per i dati contenuti nel datagramma ma solo per le informazioni contenute nell'header. I compiti di verifica e controllo del flusso dei dati sono demandati ad altri protocolli del modello a strati. (per essere precisi IP non tratta nemmeno in maniera appropriata il trasferimento dei datagrammi. IP può fare una stima del miglior instradamento per muovere il datagramma lungo la rete ma non ha alcun metodo interno di verifica che gli consenta di valutare se il percorso scelto sia il più veloce ed efficiente). Parte del sistema IP definisce come i gateway trattano i datagrammi, come e quando essi dovrebbero generare messaggi di errore, e come riparare ad errori che si dovessero presentare.

Abbiamo visto come i datagrammi possono essere spezzati in sezioni più piccole per essere trasmesse e riassemblati in una nuova locazione, un processo chiamato frammentazione e riassemblaggio. IP consente un'ampiezza massima dei pacchetti pari a 65535 byte, che è più ampia di quanto possano trattare la maggior parte dei

network, da cui la necessità della frammentazione. IP ha la capacità di suddividere automaticamente un pacchetto in frammenti più piccoli, se necessario.

Quando il primo datagramma di un messaggio più grande che è stato suddiviso in frammenti arriva a destinazione, viene attivato un timer di riassemblaggio dallo strato IP ricevente. Se non vengono ricevuti tutti i frammenti del messaggio entro il tempo in cui il timer raggiunge un valor prefissato, tutti i frammenti ricevuti vengono scartati. La macchina ricevente riconosce l'ordine in cui i pezzi ricevuti vanno riassemblati grazie ad un campo nell'header IP. Una conseguenza di questo processo è che un datagramma frammentato ha una minor probabilità di giungere a destinazione rispetto ad un datagramma non frammentato, per cui la maggior parte delle applicazioni cerca di evitare la frammentazione il più possibile.

IP non è orientato alla connessione, il che significa che non si preoccupa di quali nodi vengono attraversati dal pacchetto, o perfino in quale macchina parte il datagramma e in quale macchina arriva. Questa informazione è nell'header, ma il processo di analizzare e passare oltre un datagramma non ha nulla a che fare con il fatto che IP analizza gli indirizzi IP mittente e destinatario. IP tratta l'indirizzamento di un datagramma con gli indirizzi Internet a 32 bit, sebbene gli indirizzi di trasporto utilizzino 8 bit.

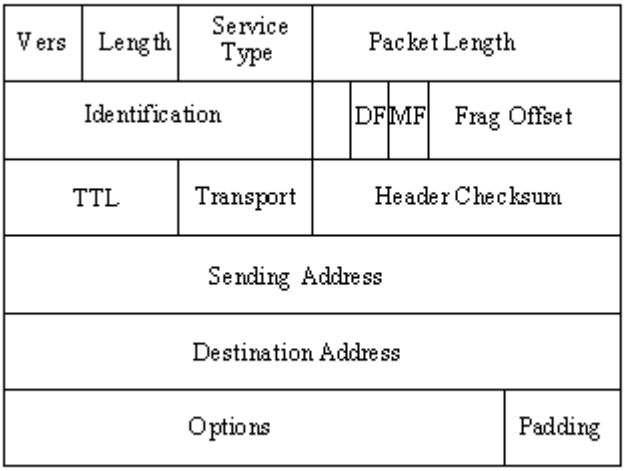
L'header del datagramma del protocollo IP

Viene la tentazione di confrontare IP con uno standard di rete hardware come Ethernet a causa delle similarità nell'impacchettamento dei dati. Ethernet assembla

un frame combinando i dati con un header contenente informazioni di indirizzamento. IP fa lo stesso eccettuato il fatto che i contenuti dell'header sono specifici di IP. Quando Ethernet riceve un pacchetto assemblato dal protocollo IP (che include l'header IP), esso aggiunge il suo header all'inizio per creare un frame, un proco chiamato incapsulamento. Una delle differenze principali tra gli header IP ed Ethernet sta nel fatto che l'header Ethernet contiene l'indirizzo fisico della macchina destinataria, mentre l'header IP contiene l'indirizzo IP. La traduzione fra i due indirizzi è effettuata dal protocollo ARP.

Il datagramma è l'unità di trasferimento utilizzata da IP, chiamata spesso datagramma IP o datagramma Internet IP vengono specificate la struttura dell'header e della coda del datagramma, organizzati in word di 32 bit. Alcuni sistemi operativi utilizzano word di lunghezza diversa sebbene la dimensione di 32 bit sia la più diffusa.

L'header IP ha una lunghezza di 6 word per un totale di 24 byte se tutti i capi opzionali sono inclusi nell'header . il più piccolo header consentito dal protocollo IP consta di 5 word per un totale di 20 byte per comprendere tutti i campi che costituiscono l'header occorre ricordare che il protocollo IP non dipende da alcun hardware ma deve poter trattare con tutte le versioni di IP che esso incontra, garantendo una piena compatibilità con le versioni precedenti del protocollo. L'organizzazione dell'header è mostrata nella figura seguente.



affronteremo nelle sezioni seguenti i vari campi.

Numero di versione

Questo è un campo a 4 bit che contiene il numero di versione del protocollo IP utilizzato. Il numero di versione del protocollo IP è richiesto cosi che il software IP ricevente sappia come decodificare la restante parte dell'header, che cambia con ogni nuova versione del protocollo. La versione più utilizzata è la 4, sebbene vari sistemi stiano testando la versione 6 (chiamata IPng).

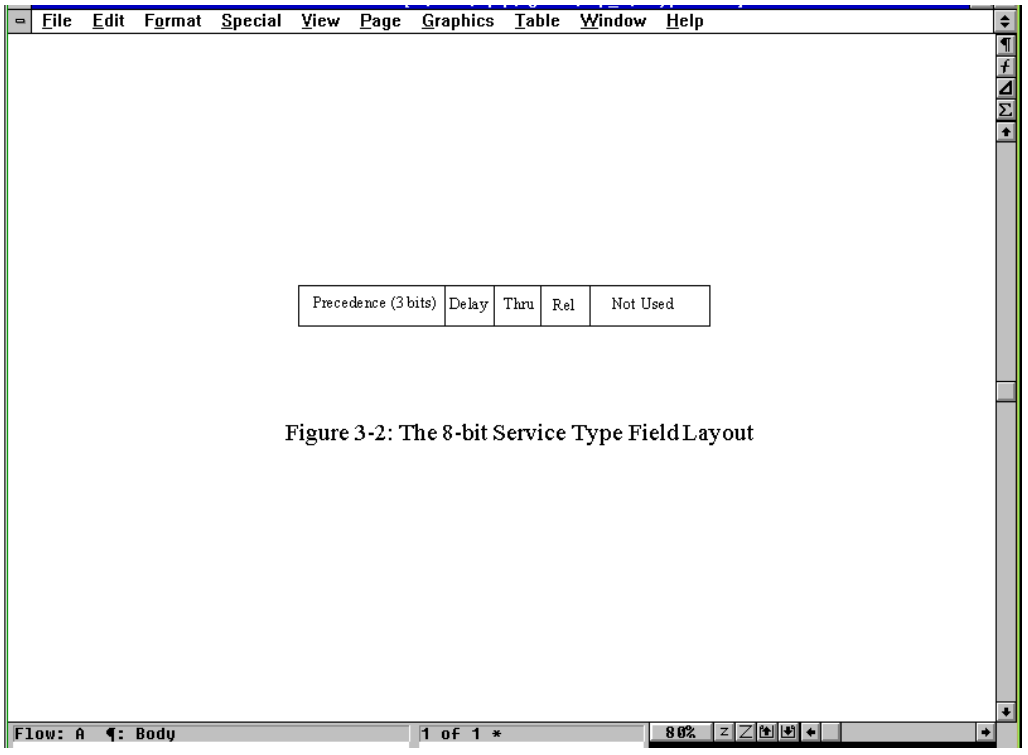
Parte delle definizioni del protocollo stabilisce che e il sofware ricevente deve analizzare per prima cosa il numero di versione dei datagrammi in arrivo prima di procedere ad analizzare il resto dell'header e i dati incapsulati. Se il sofware non può gestire la versione usata per costruire il datagramma, lo strato IP della macchina ricevente scarta il pacchetto ignorando completamente i dati.

Lunghezza dell'header (header lenght)

Questo è un campo a 4 bit che specifica la lunghezza dell'header in numero di word di 32 bit. L'header più corto possibile consta di 5 word , ma l'uso di campi opzionali può incrementare la grandezza dell'header fino ad un massimo di 6 word. Per decodificare appropriatamente l'header, IP deve saper dove finisce l'header e dove iniziano i dati. La lunghezza dell'header è usata per calcolare dove iniziano i dati nel blocco.

Tipo di servizio

Il campo da un byte Service Type istruisce IP su come deve trattare il pacchetto. Gli 8 bit del campo sono assegnati come mostrato dalla figura seguente.



I primi tre bit indicano la precedenza del datagramma , che va da 0 (normale) a 7 (controllo di rete). Più alto è il numero , più è importante il datagramma, e, almeno in

teoria, più rapidamente il datagramma dovrebbe essere instradato verso la sua destinazione. In pratica, però, la maggior parte delle implementazioni di TCP/IP è praticamente tutte le soluzioni hardware che utilizzano TCP/IP ignorano questo campo, trattando tutti i datagrammi con la stessa priorità. I successivi tre bit sono flag da un bit che controllano il ritardo, il throughput e l'affidabilità del datagramma. Un bit settato ad 1 implica basso ritardo, alto throughput e alta affidabilità rispettivamente. Gli ultimi due bit del campo non vengono utilizzati. La maggior parte di questi bit sono ignorati dalle correnti implementazioni del protocollo IP, e i datagrammi sono trattati tutti nella stessa maniera.

Lunghezza del datagramma (datagram lenght)

Questo campo fornisce la lunghezza totale del datagramma, incluso l'header, in byte. La lunghezza dell'area dati può essere calcolata sottraendo la lunghezza dell'header da questo valore. La lunghezza di questo campo è di 16 bit, da cui una lunghezza massima di 65536 byte per il datagramma

Identificazione

Questo campo contiene un numero che è un identificatore univoco creato dal nodo mittente. Questo numero è richiesto nella fase di riassemblaggio dei messaggi frammentati, assicurando che i frammenti di un messaggio non siano frammisti a quelli di un altro. Ogni pezzo di dati ricevuto dallo strato IP da uno strato di protocollo superiore riceve uno di questi codici di identificazione. Se un datagramma viene frammentato ogni frammento riceve lo stesso numero di identificazione.

Flag

IL campo Flag è a tre bit, il primo dei quali viene lasciato inutilizzato (è ignorato dal protocollo e di solito non vi viene scritto alcun valore). I due bit rimanenti sono dedicati a flag chiamati DF (Don't Fragment) e MF (More Fragment), che controllano la gestione del datagramma quando è desiderabile la frammentazione.

Se il flag DF è settato ad 1, il datagramma non può essere rammentato in alcuna circostanza. Se il software del livello IP non può mandare il datagramma ad un'altra macchina senza frammentarlo, e questo bit è settato ad 1, il datagramma viene scartato ed un messaggio di errore è inviato all'apparecchiatura mittente.

Se il flag MF è settato ad 1, il corrente datagramma è seguito da altri pacchetti (talvolta detti sottopacchetti), che devono essere riassemblati per ricreare il messaggio completo. L'ultimo frammento che viene inviato come parte di un frammento più grande ha il flag MF a 0 cosicché l'apparecchio ricevente sa quando deve smettere di attendere nuovi pacchetti. Poiché l'ordine di arrivo dei pacchetti può non corrispondere all'ordine in cui essi sono inviati, il flag MF è usato in congiunzione con il campo Fragment Offset 8 il campo successivo nell'header) per indicare alla macchina ricevente la completa estensione del messaggio.

Fragment Offset

Se il flag MF (More Fragments) è settato ad 1, indicando che si è di fronte alla frammentazione di un datagramma più grande, il fragment offset contiene la posizione all'interno del datagramma complessivo del sottomessaggio contenuto nel

datagramma attuale. Ciò permette al protocollo IP di ricomporre i vari frammenti nell'ordine appropriato. Gli offset sono sempre calcolati in relazione all'inizio del messaggio. Questo è un campo a 13 bit, poiché gli offset sono calcolati in unità di 8 byte, corrispondenti ad una lunghezza massima di 65536 byte. Usando il numero di identificazione per sapere a quale pacchetto appartiene il frammento, lo strato IP ricevente può poi usare il fragment offset per riassemblare il pacchetto.

Time To Live (TTL)

Questo campo da l'ammontare di tempo in secondi che rimane ad un datagramma in una rete prima di essere scartato. Il campo è settato dal nodo mittente quando viene assemblato il datagramma. Usualmente tale campo è settato a valori compresi fra 15 e30 secondi.

Gli standard TCP/IP stabiliscono che il campo TTL va decrementato almeno di un secondo da ogni nodo che processa il pacchetto, anche se il tempo di trattamento è inferiore al secondo. Inoltre quando un datagramma passa per un gateway, viene segnato l'istante di arrivo, cosicché se il pacchetto deve attendere per essere processato, il tempo di attesa nel gateway fa decrementare il campo TTL. In tal modo, se un gateway è particolarmente oberato e non può trattare il datagramma in un breve lasso di tempo, il timer TTL può scaricarsi nell'attesa e il datagramma viene scartato.

Se il campo TTL giunge a 0, il datagramma viene scartato ma viene inviato un messaggio al nodo mittente. In tal modo la macchina mittente può rinviare il

datagramma. Queste regole di governo del campo TTL, hanno lo scopo di impedire che datagrammi possano, per qualche problema, circolare indefinitamente all'interno della rete.

Transport Protocol

Questo campo contiene il numero di identificazione del protocollo di trasporto cui il pacchetto è stato affidato. I numeri sono definiti dal Network Information Center (NIC) che governa Internet. Ci sono al momento circa 50 protocolli di transport cui sia stato assegnato un numero identificativo. I due protocolli più importanti sono ICMP , ce ha il numero 1, e TCP che è il numero 6.

Header Checksum

Il numero in questo campo è un checksum per i dati contenuti nell'header. Poiché il campo Time To Live cambia ad ogni nodo, anche il checksum cambia ad ogni passaggio del datagramma in una nova macchina. L'algoritmo di checksum prevede l'effettuazione del complemento ad 1 della somma a 16 bit i tutte le parole a 16 bit che costituiscono l'header.

Questo è un algoritmo veloce ed efficiente, ma fallisce in alcune inusuali condizioni di corruzione dell'header come la perdita di una intera parola a 16 bit che contiene solo zeri. Comunque, poiché i campi di checksum usati sia dal protocollo TCP che dal protocollo UDP, coprono l'intero datagramma, questi tipi di errore vengono rilevati quando si riassembla l'intero pacchetto.

Sending address e destination address

Questi campi contengono gli indirizzi a 32 bit IP del mittente e del destinatario.questi campi sono fissati alla reazione del datagramma e non vengono modificati durante il percorso.

Options

Il campo Options è opzionale, composto da vari codici di lunghezza variabile . se più di una opzione viene usata nel datagramma, esse appaiono consecutivamente nell'header IP. Tutte le opzioni sono normalmente controllate da un byte che è usualmente diviso in tre campi : un flag di copia di un bit, una classe di opzione a 2 bit, e un numero di opzione a 5 bit. Il flag di copia è usato per stabilire come viene trattata l'opzione quando diviene necessaria la frammentazione in gateway. Quando il bit è settato a 0, l'opzione dovrebbe essere copiata nel primo datagramma ma non nei seguenti.. se il bit è ad 1, l'opzione deve essere copiata in tutti i frammenti.

La classe ed il numero dell'opzione indicano il tipo dell'opzione e il suo particolare valore. Al momento vi sono soltanto due classi di opzione stabilite (con solo due bit nel campo, sono possibili soltanto un massimo di 4 classi di opzione). Nella tabella l'elenco dei vari significati della classe e del numero di opzione

Option Class	Option Number	Description
0	0	Marks the end of the options list
0	1	No option (used for padding)
0	2	Security options (military purposes only)
0	3	Loose source routing

0	7	Activates routing record (adds fields)
0	9	Strict source routing
2	4	Timestamping active (adds fields)

Di particolare interesse sono le opzioni che abilitano la registrazione dell'instradamento e dei marcatori di tempo. Questi sono utilizzati per fornire una registrazione del passaggio del datagramma nella rete, utilizzabile a scopi di diagnostica. Entrambe queste opzioni aggiungono informazioni ad una lista contenuta nel datagramma

Vi sono due tipi di instradamento indicati nel campo Options: loose e strict. L'instradamento loose fornisce una serie di indirizzi IP attraverso cui deve passare la macchina, ma permette un qualsiasi percorso per giungere a questi indirizzi (usualmente gateway). L'instradamento di tipo strict non abilita deviazioni dal percorso specificato. Se il percorso non può essere seguito il datagramma viene abbandonato. Questo tipo di instradamento viene frequentemente utilizzato per testare dei percorsi ma raramente per la trasmissione di datagrammi i utenti a causa della più alta probabilità che il datagramma venga abbandonato o perso.

Padding

Il contenuto dell'area di padding (imbottitura) dipende dalle opzioni selezionate. In genere serve a far in modo che l'header sia costituito da un numero tondo di byte.

La vita di un datagramma

Per comprendere come gli strati TCP e IP lavorano per impacchettare ed inviare un datagramma, diamo un'occhiata ad una versione semplificata del passaggio di un datagramma da una macchina all'altra. Quando un'applicazione deve inviare un datagramma sulla rete, esegue alcuni semplici passi. Per prima cosa costruisce il datagramma IP con la lunghezza legale stabilita dall'implementazione locale del protocollo IP. Viene calcolato il checksum per i dati e poi viene costruito l'header IP. Poi deve essere determinata la prima macchina del percorso verso la destinazione per instradare il pacchetto verso la macchina di destinazione direttamente nella rete locale, o verso un gateway se si usa la interconnessione con altre reti. Se l'instradamento è importante questa informazione viene aggiunta all'header mediante un'opzione. Alla fine il datagramma è affidato alla rete.

Mentre il datagramma viaggia lungo l'internet, ogni gateway effettua una serie di test. Dopo che il livello di rete ha eliminato il suo proprio header, lo strato IP del gateway calcola il checksum e verifica l'integrità del datagramma. Se il checksum calcolato non corrisponde a quello presente nel datagramma, questo viene scartato e viene inviato un messaggio di errore alla macchina mittente. Poi il campo TTL viene decrementato e controllato. Se il tempo del datagramma si è esaurito, esso viene scartato ed un messaggio di errore viene inviato alla macchina mittente. Dopo aver determinato il prossimo nodo della rete, o analizzando l'indirizzo di destinazione o seguendo l'instradamento previsto nelle opzioni del datagramma contenute nel suo

header IP, il datagramma viene ricostruito con il nuovo valore TTL e il nuovo checksum.

Se la frammentazione si rende necessaria a causa di una crescita dell'ampiezza del pacchetto o di limitazioni del sofware , il datagramma viene diviso, e sono assemblati nuovi datagrammi con opportune informazioni di header. Alla fine il datagramma viene inviato al livello di rete.

Quando il datagramma giunge infine a destinazione, il sistema effettua un calcolo del checksum e, nel caso non vi siano errori, controlla se vi sono altri frammenti. Se sono richiesti altri frammenti per assemblare l'intero pacchetto, il sistema attende, attivando un timer in modo da assicurarsi che l'intero datagramma giunga in un tempo ragionevole. Se tutte le parti del messaggio originario sono arrivate ma il sistema non può riassemblarle perché il timer è giunto a zero, il datagramma viene scartato e viene inviato un messaggio di errore al mittente. Alla fine viene eliminato l'header IP, l'originale messaggio viene ricostruito se era stato frammentato, e viene inviato agli strati superiori fino allo strato di applicazione. Se è richiesta una replica, essa viene costruita e rimandata indietro.

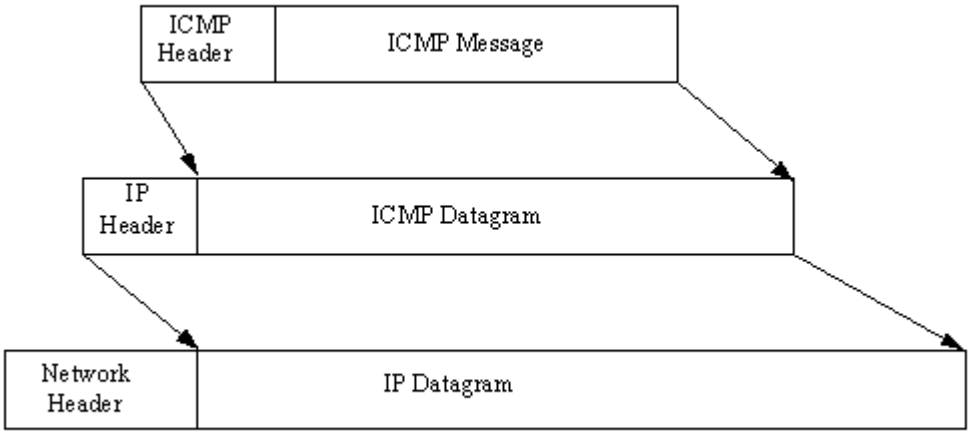
Internet Control Message Protocol

Come abbiamo visto possono sorgere molti problemi nell'instradamento di un messaggio da trasmettitore a ricevitore: il timer TTL può espirare, datagrammi frammentati possono non arrivare con tutti i segmenti intatti, un gateway può instradar in maniera non corretta un datagramma. Permettere all'apparecchiatura

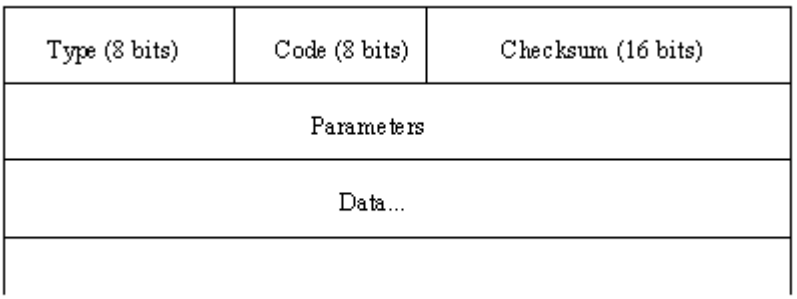
mittente di conoscere i problemi in cui è incorso il datagramma inviato è importante, come lo è il corretto trattamento degli errori occorsi durante l'instradamento. Questo è il compito del protocollo ICMP. Esso è sostanzialmente un sistema di reporting degli errori. Esso è parte integrante del protocollo IP e deve essere presente in ogni implementazione di esso. Fornisce comprensibili messaggi di errore e segnali attraverso le varie versioni del protocollo IP e i vari sistemi operativi. In sostanza ICMP è il sistema di comunicazione dello strato IP. I messaggi generati dal protocollo ICMP sono trattati dal resto della rete come ogni latro datagramma, ma sono interpretati in maniera differente dal software dello strato IP. ICMP ha un header costruito nella stessa maniera di ogni altro datagramma, e i datagrammi ICMP non sono differenziati da i normali datagrammi portatori di dati finché lo strato IP di una macchina ricevente non processa il datagramma ICMP in maniera appropriata.

Nella generalità dei casi, i messaggi di errore inviati dal protocollo ICMP sono inviati indietro alla macchina mittente del datagramma originale. Ciò perché solo gli indirizzi IP del mittente e del ricevitore sono inclusi nell'header. Poiché l'errore non ha alcun significato per la macchina destinataria, il mittente è il destinatario logico del messaggio di errore. Il mittente può poi determinare a partire dal messaggio ICMP il tipo di errore che si è avuto e stabilisce il modo migliore di rinviare il datagramma.

I messaggi ICMP subiscono due processi di incapsulamento: incorporazione in un datagramma IP e poi in un frame di rete, come mostrato nella figura seguente



gli header ICMP hanno un formato leggermente differente da quelli IP. Esso differisce inoltre secondo il tipo di messaggio di errore. Comunque tutti gli header ICMP cominciano con gli stessi tre campi: un campo tipo di messaggio, un campo codice, ed un checksum per il messaggio ICMP. La figura seguente mostra la struttura di un messaggio ICMP



normalmente un messaggio ICMP che sta facendo un rapporto su un errore di consegna include inoltre l'header e i primi 64 bit del campo dati del datagramma che ha subito l'errore. L'inclusione dei 64 bit del datagramma originale consente di compiere due cose. Prima di tutto, esso abilità la macchina mittente a confrontare il frammento di datagramma al datagramma originale. Inoltre, poiché la maggior parte

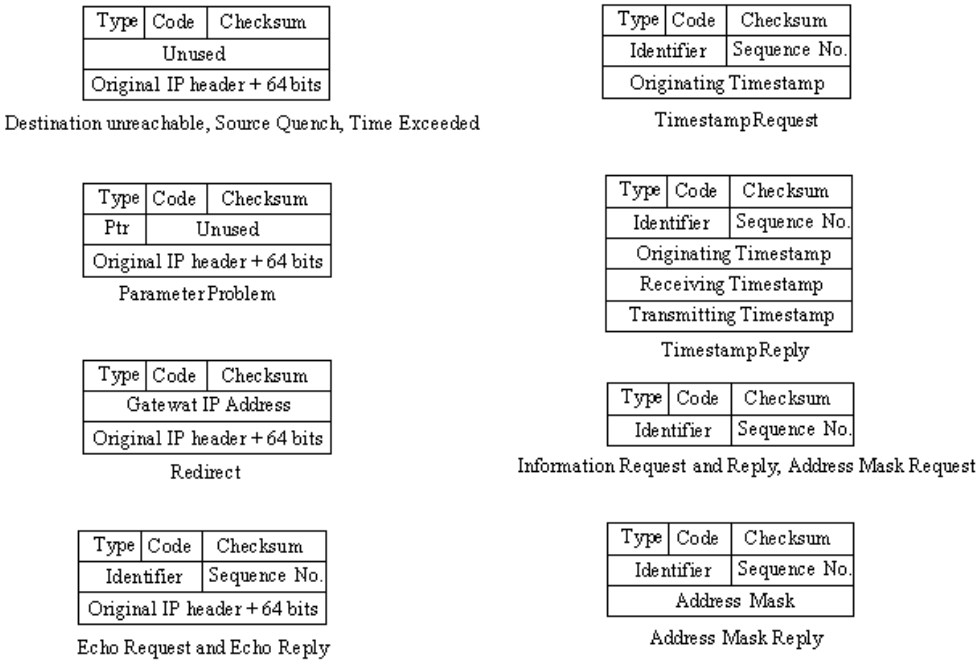
dei protocolli coinvolti è definita all'inizio del datagramma, l'inclusione del frammento del datagramma originale permette alla macchina che ha ricevuto il messaggio ICMP di effettuare vari test di diagnostica.

Il campo ad 8 bit sul tipo di messaggio presente nell'header ICMP può avere uno dei valori elencati nella tabella seguente

Value	Description
0	Echo Reply
3	Destination Not Reachable
4	Source Quench
5	Redirection Required
8	Echo Request
11	Time to Live Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request (now obsolete)
16	Information Reply (now obsolete)
17	Address Mask Request
18	Address Mask Reply

Il campo Codice fornisce ulteriori informazioni alla macchina ricevente. Il checksum nell'header ICMP è calcolato nella stessa maniera del checksum di un header IP.

L'organizzazione di un header ICMP è leggermente diversa per ogni tipo di messaggio. La figura seguente mostra i layout per ogni tipo di messaggio.



I messaggi Destination Unreachable e Time Exceeded si spiegano da soli, anche se essi sono usati anche in altre circostanze come quando il datagramma deve essere frammentato ma il flag Don’t Fragment è settato. Questo porta all’invio di un messaggio Destination Unreachable alla macchina mittente.

IL messaggio Source Quench è usato per controllare la velocità alla quale sono trasmessi i datagrammi, sebbene questa sia una forma di controllo del flusso molto rudimentale. Quando un apparecchio riceve questo messaggio, esso dovrebbe ridurre la velocità di trasmissione finché non cessano i messaggi Source Quench. Questi messaggi sono tipicamente emessi da un gateway o un host che ha o un buffer di ingresso pieno o ha rallentato il trattamento dei datagrammi in arrivo per altre cause. Se il buffer è pieno si suppone che l’apparecchio invii un messaggio Source Quench per ogni datagramma che viene scartato. Alcune implementazioni del protocollo inviano un messaggio Source Quench quando il livello di riempimento del buffer di

ingresso supera una certa percentuale per rallentare la ricezione e consentire lo svuotamento del buffer stesso.

Messaggi di redirezione sono inviati ad un gateway nel percorso quando è disponibile un instradamento migliore. Per esempio, se un gateway ha appena ricevuto un datagramma da un altro gateway ma controllando i suoi dati si rende conto che esiste un percorso migliore, manda un messaggio di redirezione all'altro gateway contenente l'indirizzo IP del percorso migliore. Quando viene inviato un messaggio di redirezione, un valore intero è posto nel campo codice dell'header per indicare le condizioni per le quali la redirezione si applica. Un valore 0 indica significa che i datagrammi per ogni apparecchio della rete di destinazione dovrebbero essere reinstradati. Un valor di 1indica che solo i datagrammi per la macchina specificata dovrebbero essere reinstradati. Un valore 2 implicano che solo i datagrammi per la rete con lo stesso tipo di servizio dovrebbero essere reinstradati. Infine un valore 3 reinstrada soltanto per lo stesso host con lo stesso tipo di servizio.

Il messaggio Parameter Problem è usato ogniqualvolta si è avuto un errore sintattico o semantico nell'header IP. Questo può accadere quando si sono utilizzate opzioni con argomenti non corretti. Quando un messaggio Parameter Problem viene inviato alla macchina mittente , il campo Parameter nel messaggio di errore ICMP contiene un puntatore al byte nell'header IP che ha causato il problema.

I messaggi echo request e reply sono comunemente utilizzati a scopi di debugging. Quando viene inviata una richiesta , un apparecchio o un gateway lungo il percorso invia una replica indietro alla macchina specificata. Questa coppia richiesta/replica è

utile per identificare problemi di instradamento, avarie dei gateway e problemi di cablaggio. Il semplice fatto di trattare un messaggio ICMP agisce come un controllo della rete. Poiché ogni gateway o apparecchio lungo il percorso deve decodificare in maniera corretta gli header e passare in avanti il messaggio.

Richieste e repliche di marcatura del tempo abilitano il monitoraggio della temporizzazione dei messaggi che passano lungo la rete. In combinazione con il routing di tipo strict , ciò può essere utile per identificare coli di bottiglia. Richieste e repliche di address mask sono usate per test in specifiche reti e sottoreti.

IPng: IP versione 6

Quando fu sviluppata la versione 4 del protocollo IP (la versione attualmente utilizzata) , l'uso di un indirizzo IP a 32 bit sembrava più che sufficiente per gestire gli usi progettati di Internet. Con l'incredibile tasso di crescita di Internate negli ultimi anni, l'indirizzo a 32 bit potrebbe diventare un problema. Per superare questo limite IP Next Generation, usualmente chiamato IP versione 6 è in via di sviluppo.

Attualmente sono allo studio diverse proposte di implementazione di IPng, le più popolari delle quali sono TUBA (TCP e UDP con indirizzi più grandi), CATNIP (Common Architecture for the Internet), e SIPP (Simple Internet Protocol Plus). Nessuno dei tre soddisfa tutti i cambiamenti proposti per la versione 6, ma un compromesso è probabile.

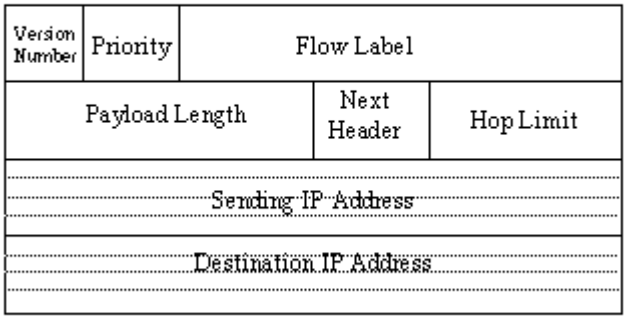
Cosa ha da offrire IPng? Di seguito la lista dei cambiamenti:

- Indirizzi a 128 bit invece di 32 bit

- Header IP più efficienti con estensioni per applicazioni ed opzioni
- Nessun checksum per l'header
- Un'etichetta di flusso per richieste di qualità del servizio
- Prevenzione di frammentazioni intermedie dei datagrammi
- Sicurezza integrata nel protocollo per autenticazione e crittografia

Datagrammi IPng

L'header dei datagrammi IPng è stato modificato rispetto a quello della versione 4. i cambiamenti sono dovuti principalmente per supportare il nuovo indirizzamento a 128 bit e rimuovere campi obsoleti e non necessari. Il layout di base dell'header IPng è mostrato nella figura seguente.



il numero di versione nell'header del datagramma IP è di 4 bit e contiene il numero di release (6 per IPng). Il campo Priorità è lungo 4 bit e contiene un valore che indica la priorità del datagramma. La priorità è utilizzata per indicare l'ordine di trasmissione. La priorità è settata prima con un'ampia classificazione , poi un identificatore più corto in ogni classe.

Il campo etichetta di flusso (Flow Label Field) è lungo 24 bit ed è ancora in fase di sviluppo. Sarà probabilmente utilizzato con l'indirizzo IP della macchina sorgente per fornire identificazioni di flusso per la rete. Per esempio, se stiamo utilizzando una workstation UNIX, il flusso sarà differente rispetto ad una macchina differente come un PC WINDOWS . questo campo può essere utilizzato le caratteristiche di flusso e fornire alcune capacità di adattamento. Il campo può essere usato anche per aiutare ad identificare le macchine target per ampi trasferimenti. , casi in cui un sistema cache diventa più efficiente nell'instradamento fra sorgente e destinazione.

Il campo Payload Lenght è un campo a 16 bit usato per specificare la lunghezza totale del datagramma in byte. La lunghezza totale non comprende l'header IP stesso. L'uso di un campo a 16 bit limita l'ampiezza del datagramma a 65536 byte. Ma c'è la possibilità di inviare datagrammi più ampi usano un header di estensione.

Il campo Next Header è usato per indicare qual header segue l'header IP quando altre applicazioni vogliono appoggiarsi sull'header IP. Diversi valori di questo campo sono mostrati nella figura seguente.

Value	Description
0	Hop-by-hop options
4	IP
6	TCP
17	UDP
43	Routing
44	Fragment
45	Interdomain Routine

46	Resource Reservation
50	Encapsulating Security
51	Authentication
58	ICMP
59	No Next Header
60	Destination Options

Il campo Hop limit determina il numero di salti fra nodi che il datagramma può effettuare. Con ogni passaggio da un nodo all'altro il campo è decrementato di 1. quando esso assume il valore 0, il datagramma è scartato.

Classificazione della priorità

Il campo Priorità Classification nell'header IPng divide il datagramma in due categorie: a congestione controllata e a congestione non controllata. I datagrammi a congestione non controllata sono sempre instradati con priorità superiore ai datagrammi a congestione controllata. Vi sono sottocategorie di classificazione dei datagrammi senza controllo di congestione ma non sono ancora diventate standard.

Se il datagramma è a controllo di congestione , esso è sensibile a problemi di congestione nella rete. Se si ha congestione , il datagramma viene rallentato e conservato temporaneamente in una cache finché il problema si allevia. All'interno della categoria dei datagrammi a congestione controllata vi sono diverse sottoclassi che precisano il tipo di priorità. Le sottocategorie sono mostrate nella tabella seguente.

Value	Meaning
0	No priority specified
1	Background traffic
2	Unattended data transfer
3	Unassigned
4	Attended bulk transfer
5	Unassigned
6	Interactive traffic
7	Control traffic

Il traffico di informazioni per l'instradamento e controllo della rete ha la priorità più alta (7). Applicazioni interattive come Telnet hanno la priorità di traffico interattivo 86). Trasferimenti che sono critici dal punto di vista temporale ma sono ancora controllati da un'applicazione interattiva come gli FTP hanno una categoria 4. le e-mail hanno usualmente una categoria 2.

Etichette di flusso

Il campo Flow Label può essere utilizzato per aiutare ad identificare mittente e destinatario di molti datagrammi IP. Impiegando delle cache per controllare i flussi, i datagrammi possono essere instradati in maniera più efficiente. Non tutte le applicazioni possono gestire le etichette di flusso, nel qual caso il loro valore è posto a zero.

Un semplice esempio può aiutare a mostrare l'utilità delle etichette di flusso. Supponiamo che un PC windows è collegato ad un server Unix su un'altra rete e sta inviando un gran numero di datagrammi. Settando uno pacifico valore per l'etichetta

di flusso per tutti i datagrammi relativi a quella trasmissione, i router lungo il percorso possono creare delle registrazioni nelle loro cache di instradamento che indicano la strada lungo la quale devono instradare i pacchetti con quell'etichetta di flusso. Quando arrivano successivi datagrammi con la medesima etichetta di flusso , i router non devono ricalcolare il percorso di instradamento. Ciò accelera il passaggio dei datagrammi attraverso i router.

Per impedire che le cache crescano troppo o contengano informazioni che mandano in stallo il sistema, il protocollo IPng prevede che una cache non possa essere mantenuta da un router più di 6 secondi. Se un nuovo datagramma con lo stesso campo flow label non è ricevuto entro 6 secondi, la relativa registrazione della cache viene rimossa. Per impedire equivoci relativi all'utilizzo ripetuto dello stesso valore di flow label, la macchina mittente deve aspettare 6 secondi rima di poter riutilizzare lo stesso valore di flow label per una nuova destinazione.

Il protocollo IPng permette di utilizzare le flow label anche per poter riservare un percorso di instradamento per applicazioni in cui il tempo è un fattore critico. Per esempio, un'applicazione real time che deve mandare diversi datagrammi lungo la stessa rete e necessità di una trasmissione più rapida possibile può stabilire il percorso di instradamento inviando datagrammi in anticipo, facendo attenzione a non superare di time out di 6 secondi dei router intermedi.

Indirizzi a 128 bit.

Probabilmente la più importante capacità del protocollo IPng è quella di fornire indirizzi IP più lunghi., passando da 32 a 128 bit. Ciò permette di assemblare un numero incredibile di indirizzi, probabilmente più di quanti se ne potranno mia usare.

Il nuovo tipo di indirizzamento supporta tre tipi di indirizzi: unicast, muticast, anycast.

- Gli indirizzi unicast sono pensati per identificare una particolare interfaccia di una macchina . questo consente ad esempio ad un PC di avere molti protocolli in uso, ciascuno con il suo indirizzo IP
- Un indirizzo multicast identifica un gruppo di interfacce, abilitando tutte le macchine del gruppo a ricevere lo stesso messaggio. E' simile all'indirizzamento broadcast della versione 4 ma con maggiore flessibilità nella definzione dei gruppi. Una interfaccia di una macchina potrebbe appartenere a più gruppi.
- Un indirizzo anycast identifica un gruppo di interfacce in un singolo indirizzo multicast. In sostanza più di una interfaccia possono ottenere il datagramma sulla stessa macchina.

Anche la gestione della frammentazione e del riassemblaggio sono cambiati nel protocollo IPng. E' stato proposto inoltre per tale protocollo uno schema di autenticazione in grado di assicurare che i dati non sono stati corrotti nel percorso fra mittente e destinatario. , e di assicurare inoltre che la macchina mittente è chi afferma di essere.

IP Extension Header

IPng permette di attaccare header addizionali all'header IP. Questo potrebbe essere necessario quando non è possibile un semplice instradamento verso la destinazione, o quando servizi speciali come l'autenticazione sono richiesti per quel datagramma. L'informazione addizionale richiesta è impacchettata in un header di estensione e aggiunta all'header IP.

IPng identifica diversi tipi di header di estensione individuati da un numero posto campo Next Header dell'header IP. Diverse estensioni possono essere attaccate allo stesso header IP, con ogni campo Next extension che indica il tipo dell'estensione successiva. Normalmente gli header sono collegati n ordine numerico crescente. Ciò facilita i router nell'analizzare le estensioni, smettendo quando supera le estensioni che sono di sua competenza.

Hop-by-hop header

Il tipo di estensione 0 è l'hop-by-hop usato per fornire informazioni IP ad ogni macchina attraverso la quale passa il datagramma. Le opzioni contenute nell'estensione hop-by-hop hanno un formato standard costituito da un valore di tipo, una lunghezza, ed un campo valore (fatta eccezione per l'opzione Pad1, che ha un valor singolo settato a zero e non ha i campi lunghezza e valore). I campi di lunghezza e valore sono di un byte, mentre la lunghezza del campo valore è variabile ed indicata dal campo lunghezza.

Vi sono tre tipi di estensioni hop-by-hop definite fin'ora, chiamate Pa1,PadN e Jumbo Payload. L'opzione Pad1 è un singolo valore posto a zero senza campi lunghezza e valore. Essa è usata per alterare l'ordine e la posizione di altre opzioni nell'header quando necessario, variazioni dettate usualmente da un'applicazione. L'opzione PadN è simile fatta eccezione per il fatto che essa ha N zeri nel campo valore ed un valore calcolato per la lunghezza.

L'estensione Jumbo Payload è usata per gestire datagrammi di ampiezza superiore a 65536 byte. Il campo lunghezza nell'header IP è limitato a 16 bit da cui il mite di 65536 byte per la lunghezza del datagramma. Per gestire ampiezze superiori, il campo lunghezza dell'header IP è posto a 0, il che redirezione il router a cercare nell'estensione la corretta lunghezza del datagramma. IL campo lunghezza può essere nell'header di estensione che usa 32 bit, il che significa poter giungere a 4 gigabyte.

Routing Headers

Un'estensione di instradamento può essere agganciata all'header IP quando la macchina mittente vuole controllare l'instradamento del datagramma piuttosto che lasciare il compito ai router presenti lungo il percorso. L'estensione di routing può essere utilizzata per dare un percorso fino alla destinazione fiale. L'estensione di routing include campi per ogni indirizzo IP lungo la rotta desiderata.

Header di frammento

Possono essere attaccati all'header IP per abilitare una macchina a frammentare un datagramma in parti più piccole. Parte del disegno del protocollo IPng è stata

dedicata ad evitare frammentazioni successive, ma in alcuni casi, la frammentazione deve essere abilitata per poter trasmettere il datagramma lungo il network.

Header di autenticazione

L'header di autenticazione è usato per assicurare che non vi è stata alterazione dei contenuti del datagramma e che il datagramma è stato effettivamente originato dalla macchina il cui indirizzo appare nell'header IP. Per default IPng utilizza uno schema di autenticazione chiamato Message Digest 5 (MD5). Altri schemi di autenticazione possono essere utilizzati se entrambi i capi della comunicazione sono d'accordo sullo stesso schema.

L'header di autenticazione consiste di un indice dei parametri di sicurezza (SPI) che, quando in combinazione con l'indirizzo IP del destinatario, definisce lo schema di autenticazione,. L'SPI è seguito dai dati di autenticazione, che con MD5 sono lunghi 16 byte. MD5 parte con una chiave (con caratteri di riempimento fino a formare un totale di 128 bit se è più corta di questo numero), poi accoda l'intero datagramma. La chiave è poi etichettata alla fine , e l'algoritmo MD5 viene seguito sull'intero pacchetto. Per prevenire problemi coni contatori di hop e lo stesso header di autenticazione che alterano i valori, essi sono azzerati prima di calcolare il valore di autenticazione. L'algoritmo MD5 genera un valore a 128 bit che è piazzato nell'header di autenticazione. Questi passi vengono compiuti in ordine inverso in ricezione. Naturalmente perché tutto sia a posto le macchine terminali devono avere la stessa chiave.

I contenuti del datagramma possono essere criptati prima della generazione del valore di autenticazione usando lo schema di crittografia di default di IPng, chiamato Cipher Block Chaining (CPI).